UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/780,407	02/17/2004	Ron Ben-Natan	GRD03-04	1295

7590 09/01/2006

Barry W. Chapin, Esq.
CHAPIN & HUANG, L.L.C.
Westborough Park Drive
1700 West Park Drive
Westborough, MA 01581

EXAMINER	
STEVENS, ROBERT	

ART UNIT	PAPER NUMBER
2162	

DATE MAILED: 09/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/780,407	BEN-NATAN, RON	
	Examiner	Art Unit	
	Robert Stevens	2162	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 February 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Drawings

1. The Office objects to figures 5-8.

2. The drawings are objected to because they do not clearly indicate how Figures 5, 6, 7 and 8 interconnect. One way to indicate an interconnection between the flow charts of two figures is to end the first figure's flow chart with an arrow from the last flow chart element to a circle containing the letter "A", then begin the second figure's flow chart with an arrow from a circle containing the letter "A" to first the flow chart element of the second figure. Subsequent figure interconnections would use the letter "B", and so on. For another alternative, refer to Figures 6A and 6B of Patent No. 6,687,702.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New

Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

3. The abstract of the disclosure is objected to because of a minor informality. The first sentence is a fragment. It appears that Applicant intended to end this sentence with the word "overhead". Correction is required. See MPEP § 608.01(b).

4. Applicant is reminded to update the status the cross references to related applications (i.e., update status, add serial number/patent number, remove docket number, etc.), as found from page 9 line 31 through page 10 line 3. Correction is required.

5. The specification is object to for the following informalities: Page 11 line 25 states "the IPC intercept 134". This reference number 134 does not agree with Figure 1, which uses reference number 140. Applicant is reminded to correct all spelling/grammar/etc. errors throughout the disclosure. Correction is required.

Claim Objections

6. Claim 25 is objected to because of the following informalities: The 8th line of claim 18 ("of a pending ...") is not terminated with a semicolon. Appropriate correction is required.

Claim Rejections - 35 USC § 101

7. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

8. **Claims 1-17, 21-37 and 39-41 are rejected under 35 U.S.C. 101** because the claimed invention is directed to non-statutory subject matter.

To be statutory, a claimed computer-related process must either: (A) result in a physical transformation outside the computer for which a practical application is either disclosed in the specification or would have been known to a skilled artisan, or (B) be limited to a practical application with useful, concrete and tangible result.

Regarding independent claim 1: This claim does not produce a useful result. The method steps merely transfer data. It is noted that the preamble indicates that access monitoring is to take place, but no monitoring step (which would use the transferred data) has been recited in the body of the claim.

Regarding independent claim 21: This claim is directed to software per se. As such, it is not tangibly embodied.

Claims 1 and 21, and other claims that depend on them, are not patent eligible because the invention recited therein is not tangibly incorporated in a computer readable medium.

Independent claims 39-41 are substantially similar to claim 1, and are therefore likewise rejected, as being non-statutory because they produce no useful result.

Independent claim 40, additionally, is directed to a signal. Current Office policy is that an information carrier is not considered a tangible embodiment. One way to correct the claim language is to recite the storage of the claimed subject matter on a computer readable medium.

Claim Rejections - 35 USC § 112

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. **Claims 13-16 and 33-36 are rejected under 35 U.S.C. 112, second paragraph**, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 13: The terminology "substantially insignificant" cannot be quantified. Such terminology, therefore, renders the scope of the claim indeterminable.

Regarding claim 14: The language "depending on a data security decision" renders the scope of the claim indeterminable, because it is unclear how the claim "depends on a data security decision".

Claims 15-16 are dependent upon claim 14, and are therefore likewise rejected.

Claims 33-36 are substantially similar to claims 13-16, respectively, and are therefore likewise rejected.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. **Claims 1-41 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Krack et al. (US Patent No. 6,941,369, filed Jul. 20, 2000 and issued Sep. 6, 2005, hereafter referred to as "Krack") in view of Jai Sundar Balasubramaniyan et al.,("An Architecture for Intrusion Detection Using Autonomous Agents", 14th Annual Computer Security Applications Conf. Proc., Phoenix, AZ, Dec. 7-11, 1998, pp. 13-24, hereafter referred to as "Balasubramaniyan").

Regarding independent claim 1: Krack discloses ***A method of monitoring access to a protected database resource*** (See Krack Figure 3B, especially #33 and 34, showing an access control manager for a database.) ***comprising: identifying an attempt to access the database resource, the access attempt being local and directed to an access gateway of the database resource;*** (See Krack Figure 3B, especially #30, in context of column 6 lines 3-7.) ***intercepting the identified attempt to access the database resource, intercepting occurring in a prioritized manner with respect to receipt of the access attempt by the access gateway;*** (See Krack column 6 lines 29-33 discuss the interception of a database access request and column 7 lines 47-57, discussing the processing of multiple requests, it having been implicit that a prioritization scheme was necessary to handle simultaneous requests.) ***and transmitting, in a nondestructive manner, the intercepted access attempt, the nondestructive manner operable to preserve the intercepted access attempt for***

successive receipt by the access gateway. (See Krack column 6 lines 3-15, discussing the spawning of a daemon process and the nondestructive use of a unique cookie identifying the accessing party.)

Although Krack discloses the use of daemon processes, Krack does not explicitly disclose the use of agents. Balasubramaniyan, though, discloses: **the use of agents** (See Balasubramaniyan page 6 "2.2.1 Agents"; Figures 1 and 2 of page 17, showing the connection paths agents, monitors and users; and the 2nd-4th paragraphs under section "2.4.2 Audit Router" of page 19, discussing agent use in an intrusion detection environment.)

It would have been obvious to one of ordinary skill in the art at the time of the invention to apply the teachings of Balasubramaniyan for the benefit of Krack, because to do so allowed a system designer to add functionality to or remove functionality from an existing intrusion detection system without altering other system components, as taught by Balasubramaniyan on page 14 section 1.4.1 entitled "How the Use of Autonomous Agents Can Improve the Characteristics of an IDS". These references were all applicable to the same field of endeavor, i.e., access control of network-based systems.

Regarding claim 2: Krack teaches database access and communication with a local security device. (See Krack column 9 lines 34-40, discussing access using a proprietary database call, and Figure 3B, especially #33 and 34, showing an access control manager for a database.)

Although Krack discloses the use of daemon processes, Krack does not explicitly disclose the use of agents. Balasubramaniyan, though, discloses the use of agents (See Balasubramaniyan page 6 "2.2.1 Agents"; Figures 1 and 2 of page 17, showing the connection paths agents, monitors and users; and the 2nd-4th paragraphs under section "2.4.2 Audit Router" of page 19, discussing agent use in an intrusion detection environment.)

Regarding claim 3: Krack teaches database access, prioritized requests and non-destructive reading of those requests. (See Krack Figure 3B in the context of column 9 lines 34-40, teaching access using a proprietary database call; column 7 lines 47-57, discussing the processing of multiple requests, it having been implicit that a prioritization scheme was necessary to handle simultaneous requests; and, column 6 lines 3-15, discussing the spawning of a daemon process and the nondestructive use of a unique cookie identifying the accessing party.)

Regarding claim 4: Krack discloses establishing an IPC connection prior to receiving the IPC communication. (See Krack column 8 lines 37-38, discussing the establishment of a socket-based connection to the ACM, it having been implicit that the communications path was established before sending data via that path.)

Regarding claim 5: Krack discloses establishing connection aggregating access attempts. (See Krack column 4 lines 55-91, discussing the handling of multiple communication requests.)

Regarding claim 6: Krack discloses rerouting access attempts. (See Krack column 6 lines 3-11, discussing the spawning of daemon processes to process access attempts.)

Regarding claim 7: Krack discloses reception of access attempts for a DB server locally and remotely via a common appliance. (See Krack Figure 3B showing a gateway device #24a and and application cgi process #35 interfacing to an access control manager #33.)

Regarding claim 8: Krack discloses event processing, instruction registers, DB instructions and transmission to a security device. (See Krack column 6 lines 3-11 in the context of column 7 lines 9-17, teaching forking a process upon a request event sent via a message data structure. See column 9 lines 34-40, teaching access using a proprietary database call. See Figure 3B, showing a connection to an access control manager device #33.)

Regarding claim 9: Krack discloses establishing an IPC connection prior to receiving the IPC communication and a common access point. (See Krack column 8 lines 37-38, discussing the establishment of a socket-based connection to the ACM, it having been implicit that the communications path was established before sending data via that path. See also Figure 3B showing a gateway device #24a and and application cgi process #35 interfacing to an access control manager #33.)

Regarding claim 10: Krack discloses identifying a plurality of access paths and a common access point. (See Krack column 4 lines 55-91, discussing the handling of multiple communication requests, those requested impliedly originating from a variety of sources and coming from a avriety of communications paths. See also Figure 3B showing a gateway device #24a and and application cgi process #35 interfacing to an access control manager #33.)

Regarding claims 11-12: Krack discloses interprocess communications. (See Krack column 6 lines 3-15, discussing the spawning of a daemon process.)

Regarding claim 13: Krack discloses access interception, transmission to a security device and little effect on a host. (See Krack Figure 3B in the context of column 9 lines 34-40, teaching access using a proprietary database call. See also column 4 lines 49-54, discussing the system architecture's cost advantage over the prior art.)

Regarding claims 14-16: Krack discloses blocking an access request, then unblocking depending on a security decision, transmission of a decision, and logging. (See Krack Figure 3B, especially #33 and 34, showing an access control manager for a database, and column 4 lines 58-61, disclosing the use of a firewall. See also column 11 line 30, teaching logging options.)

Regarding claim 17: Krack discloses event processing for an IPC mechanism. (See Krack column 6 lines 3-15, discussing event processing for a request, which triggers the establishment of an IPC mechanism in the form of a socket.)

Although Krack discloses the use of daemon processes, Krack does not explicitly disclose the use of agents. Balasubramaniyan, though, discloses the use of agents. (See Balasubramaniyan page 6 "2.2.1 Agents"; Figures 1 and 2 of page 17, showing the connection paths agents, monitors and users; and the 2nd-4th paragraphs under section "2.4.2 Audit Router" of page 19, discussing agent use in an intrusion detection environment.)

It would have been obvious to one of ordinary skill in the art at the time of the invention to apply the teachings of Balasubramaniyan for the benefit of Krack, because to do so allowed a system designer to add functionality to or remove functionality from an existing intrusion detection system without altering other system components, as taught by Balasubramaniyan on page 14 section 1.4.1 entitled "How the Use of Autonomous Agents Can Improve the Characteristics of an IDS". These references

were all applicable to the same field of endeavor, i.e., access control of network-based systems.

Regarding independent claim 18: Krack discloses ***A method of controlling local access to a database*** (See Krack Figure 3B, especially #33 and 34, showing an access control manager for a database.) ***comprising: identifying a local access gateway to the database, the access gateway being a common access point into the database;*** (See Krack Figure 3B, especially #33 and 34, showing an access control manager for a database.) ***establishing an interception wrapper between a local client and the access gateway;*** (See Krack column 7 lines 9-12, discussing packetizing the message.) ***intercepting, via the interception wrapper, an access attempt from a local client prior to receipt of the access attempt by the access gateway, the access attempt indicative of a pending DB instruction in an IPC buffer identifying a local event object corresponding to the access attempt;*** (See Krack column 6 lines 3-11, discussing IPC processing.) ***indexing a notification list corresponding to the identified local event object;*** (See Krack column 6 lines 23-26, discussing the user database.) ***traversing the indexed notification list, the notification list including entries of notifications to be performed upon occurrence of the event;*** (See Krack column 6 lines 23-26, discussing reading from the user database.) ***reading a traversed entry;*** (See Krack column 6 lines 23-26, discussing reading from the user database.) ***retrieving, in response to the***

notification, the DB instruction from the IPC buffer; (See Krack column 9 lines 34-40, discussing access using a proprietary database call, and Figure 3B, especially #33 and 34, showing an access control manager for a database.) ***transmitting the retrieved DB instruction from the IPC buffer to a data security device operable to analyze the propriety of the DB instruction;*** (See Krack column 9 lines 34-40, teaching access using a proprietary database call. See Figure 3B, showing a connection to an access control manager device #33, and column 6 lines 11-21, discussing authentication.) ***reading a successive traversed entry corresponding to the access gateway, the entry indicative of the location of the access gateway;*** (See Krack column 7 lines 47-56, discussing multiple requests.) ***and notifying the access gateway of the IPC event occurrence using the read location of the access gateway.*** (See Krack column 6 lines 17-26, discussing user validation.)

Although Krack discloses the use of daemon processes, Krack does not explicitly disclose the use of agents. Balasubramaniyan, though, discloses: ***reading a traversed entry corresponding to the local agent, the entry indicative of the location of the local agent; notifying the local agent using the read location of the local agent*** (See Balasubramaniyan page 6 "2.2.1 Agents"; Figures 1 and 2 of page 17, showing the connection paths agents, monitors and users; and the 2nd-4th paragraphs under section "2.4.2 Audit Router" of page 19, discussing agent use in an intrusion detection environment.)

It would have been obvious to one of ordinary skill in the art at the time of the invention to apply the teachings of Balasubramaniyan for the benefit of Krack, because

to do so allowed a system designer to add functionality to or remove functionality from an existing intrusion detection system without altering other system components, as taught by Balasubramaniyan on page 14 section 1.4.1 entitled "How the Use of Autonomous Agents Can Improve the Characteristics of an IDS". These references were all applicable to the same field of endeavor, i.e., access control of network-based systems.

Regarding claim 19: Krack discloses event processing, an IPC mechanism and storage. (See Krack column 6 lines 3-11 in the context of column 7 lines 9-17, teaching forking a process upon a request event sent via a message data structure. See column 9 lines 34-40, teaching access using a proprietary database call. See Figure 3B, showing a connection to an access control manager device #33. See Krack column 6 lines 3-15, discussing the spawning of a daemon process. See also Figure 3B, #36, showing local data storage.)

Regarding claim 20: Krack discloses message reception, processing and transmission. (See Krack column 7 lines 9-17, discussing message processing, it having been implicit that such messages were also received and transmitted.)

Claims 21-37 are directed to agents that implement the methods of claim 1-16, respectively. As such, these claims are substantially similar to claims 1-16, and therefore likewise rejected.

Regarding independent claim 38: Krack discloses ***A data security device for monitoring access to a protected database resource*** (See Krack Figure 3B, especially #33 and 34, showing an access control manager for a database.) ***comprising: a memory;*** (See Krack Figure 3B, it having been implicit that a memory was necessary to store the code for daemon process #32.) ***a processor operable to execute instructions in the memory;*** (See Krack Figure 3B, it having been implicit that a processor was used to run the executable daemon process #32.) ***an interface operable for interconnection with a database host, the data security device in communication with the database host,*** (See Krack Figure 3B, especially #33 and 34, showing an access control manager for a database.) ***identify an attempt to access the database resource, the access attempt being local and directed to an access gateway of the database resource;*** (See Krack Figure 3B, especially #30, in context of column 6 lines 3-7.) ***intercept the identified attempt to access the database resource, intercepting occurring in a prioritized manner with respect to receipt of the access attempt by the access gateway;*** (See Krack column 6 lines 29-33 discuss the interception of a database access request and column 7 lines 47-57, discussing the processing of multiple requests, it having been implicit that a prioritization scheme was necessary to handle simultaneous requests.) ***and transmit, in a nondestructive***

manner, the intercepted access attempt, the nondestructive manner operable to preserve the intercepted access attempt for successive receipt by the access gateway. (See Krack column 6 lines 3-15, discussing the spawning of a daemon process and the nondestructive use of a unique cookie identifying the accessing party.)

Although Krack discloses the use of daemon processes, Krack does not explicitly disclose the use of agents. Balasubramaniyan, though, discloses: **the use of agents** (See Balasubramaniyan page 6 "2.2.1 Agents"; Figures 1 and 2 of page 17, showing the connection paths agents, monitors and users; and the 2nd-4th paragraphs under section "2.4.2 Audit Router" of page 19, discussing agent use in an intrusion detection environment.)

It would have been obvious to one of ordinary skill in the art at the time of the invention to apply the teachings of Balasubramaniyan for the benefit of Krack, because to do so allowed a system designer to add functionality to or remove functionality from an existing intrusion detection system without altering other system components, as taught by Balasubramaniyan on page 14 section 1.4.1 entitled "How the Use of Autonomous Agents Can Improve the Characteristics of an IDS". These references were all applicable to the same field of endeavor, i.e., access control of network-based systems.

Independent claims 39-41 are respectively directed to a computer program product, a signal, and a device for the implementation of claim 1, and as such are likewise rejected.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Non-patent Literature

Jones, Katherine, "Secure Internet Access to SAP's R/3: Keeping Dragons Out", Int. J. Network Mgmt., Vol. 8, © 1998, pp. 191-199.

Joshi, James B. D., et al., "Security Models for Web-Based Applications", Communications of the ACM, Vol. 44, No. 2, Feb. 2001, pp. 38-44.

Muller, Nathan J., "Improving Network Operations With Intelligent Agents", Int. J. Network Mgmt., Vol. 7, © 1997, pp. 116-126.

Jaeger, T., et al., "Flexible Access Control Using IPC Redirection", Proc. of the 7th Workshop on Hot Topics in Operating Systems, Mar. 29-30, 1999, pp. 191-196.

Roscheisen, Martin, et al., "A Communication Agreement Framework for Access/Action Control", 1996 IEEE Symposium on Security and Privacy, © 1996, pp. 154-163.

Appenzeller, Guido, et al., "User-Friendly Access Control for Public Network Ports", IEEE 0-7803-5417-6/99, © 1999, pp. 699-707.

US Patent Application Publications

Buchsbaum et al	2005/0086529
Brady et al	2004/0260947
Miller et al	2004/0111623
Tarquini et al	2003/0084328
Hasan et al	2003/0028624
Tarquini et al	2003/0084320
Mattsson et al	2002/0066038
Dubois et al	2002/0154646

US Patents

Vaitheeswaran et al	6,687,702

Contact Information

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Robert Stevens whose telephone number is (571) 272-4102. The examiner can normally be reached on M-F 6:00 - 2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John E. Breene can be reached on (571) 272-4107. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Robert Stevens
Examiner
Art Unit 2162

August 17, 2006

SHAHID ALAM
PRIMARY EXAMINER